Docket No.: 0054-0236P Page 2

## AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A cryptographic apparatus comprising:

plaintext packet receiver for receiving packet data transmitted and received

between terminals;

a fragmentation determination unit for making a determination as to whether

there is a need for fragmentation of the packet data by computing the packet length

when the packet data is encrypted and by comparing the computed packet length with a

predetermined packet length;

a fragmentation unit for dividing the packet data into a plurality of divided data

groups if it is determined that there is a need for fragmentation of the packet data as a

result of said determination, said fragmentation unit setting the divided data groups in a

plurality of divided data packets of a predetermined data structure capable of being

reconstructed in a transmission destination terminal, said fragmentation unit adding, to

each divided data packet, control information for ensuring continuity between the

divided data packets;

an encryption unit for separately encrypting the plurality of divided data packets

to form a plurality of encrypted packets; and

an encrypted packet transmitting unit for transmitting the plurality of encrypted

packets to the transmission destination terminal;

wherein the divided data packets include two or more associated divided data

packets and the control information permits the associated divided data packets to be

Application No. 09/898,024
Preliminary Amendment dated November 28, 2005

Docket No.: 0054-0236P

Page 3

decrypted independently without waiting for the arrival of any other associated divided

data packet.

2. (Original) A cryptographic communication system in which packet data

transmitted and received between terminals is encrypted by a transmitting-side

cryptographic apparatus and is decrypted by a receiving-side decryption apparatus; said

system comprising:

a cryptographic apparatus according to Claim 1;

a decryption apparatus which receives the plurality of encrypted packets

transmitted from said cryptographic apparatus, separately decrypts each of the plurality

of encrypted packets into the divided data packet, and transmits the plurality of divided

data packets to a transmission destination terminal in the decryption order; and

a terminal which receives the plurality of divided data packets and reconstructs

the divided data groups on the basis of the control information added to each divided

data packet to obtain the packet data.

3. (New) A cryptographic communication system according to Claim 1 wherein the

second and any subsequent divided data packet includes an additional IP header.

4. **(New)** A cryptographic method, comprising:

receiving packet data transmitted and received between terminals;

DRA/RJM/slb

Docket No.: 0054-0236P

Page 4

making a determination as to whether there is a need for fragmentation of the

packet data by computing the packet length when the packet data is encrypted and by

comparing the computed packet length with a predetermined packet length;

dividing the packet data into a plurality of divided data groups if it is determined

that there is a need for fragmentation of the packet data as a result of said

determination, setting the divided data groups in a plurality of divided data packets of a

predetermined data structure capable of being reconstructed in a transmission

destination terminal, adding, to each divided data packet, control information for

ensuring continuity between the divided data packets;

encrypting separately the plurality of divided data packets to form a plurality of

encrypted packets; and

transmitting the plurality of encrypted packets to the transmission destination

terminal:

wherein the divided data packets received at the transmission destination

terminal include two or more associated divided data packets and the control

information permits the associated divided data packets to be decrypted independently

without waiting for the arrival of any other associated divided data packet.

5. (New) A cryptographic method in which packet data transmitted and received

between terminals is encrypted according to Claim 1, and is decrypted; said method

further including:

receiving the plurality of encrypted packets;

DRA/RJM/slb

Docket No.: 0054-0236P

Page 5

decrypting separately each of the plurality of encrypted packets into the divided data packet,

transmitting the plurality of divided data packets to a transmission destination terminal in the decryption order;

receiving the plurality of divided data packets, and

reconstructing the divided data groups on the basis of the control information added to each divided data packet to obtain the packet data.

6. **(New)** A cryptographic method according to Claim 4 wherein the second and any subsequent divided data packet includes an additional IP header.